



Interview Summary: FINTRAC Panel (Sarah Paquet, Barry MacKillop, Annette Ryan, Donna Achimov)

This witness summary should be read in conjunction with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)'s institutional report.

The panel members were interviewed on September 1, 2022, by Shantona Chaudhury, Daniel Sheppard, and Dahlia Shuhaibar. Questions relating to this summary should be directed to Ms. Shuhaibar. Text contained in [square brackets] are explanatory notes provided by Commission counsel to assist the reader. Certain documents are referred to in the footnotes to assist the reader, but in many cases they were not shown to or discussed with the panel at the interview.

Background

FINTRAC is a federal agency created under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (“*PCMLTFA*”) and is Canada’s financial intelligence unit. FINTRAC collects, analyses, assesses and discloses information in order to assist in the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while protecting the personal information under its control.

Among other functions, FINTRAC receives financial transaction reports from a number of entities (such as financial institutions, casinos, and real estate professionals, which are collectively known as “reporting entities”). These reports are analyzed and assessed by FINTRAC’s Intelligence Sector, along with information FINTRAC receives from police, government departments and agencies, and members of the public (“voluntary information records” (VIRs)), to determine whether one or more of the statutory disclosure thresholds set out in the *PCMLTFA* is met. When specific statutory thresholds are met, FINTRAC is required to make “disclosures” of financial intelligence to law enforcement, the Canadian Security Intelligence Service (“CSIS”), and other departments and agencies listed in the *PCMLTFA*. Separately, FINTRAC’s Compliance Sector ensures that persons and entities with obligations under the *PCMLTFA* comply with the Act and its regulations.

The federal Department of Finance (“Finance”) is responsible for the policy direction of FINTRAC.¹

Sarah Paquet is the Director and Chief Executive Officer of FINTRAC. She was appointed to that position on November 18, 2020. Prior to joining FINTRAC, she worked

¹ For more background information about FINTRAC’s role and operations, see its institutional report.



in the public sector for 25 years, including at Justice Canada and Shared Services Canada.

Barry MacKillop is Deputy Director of Intelligence. He is responsible for the aspect of FINTRAC's mandate relating to *tactical* intelligence—that is, intelligence relating to specific individuals or entities. His sector analyses the various financial transaction reports made by reporting entities as well as VIRs, to determine whether the statutory thresholds in the *PCMLTFA* are met, requiring FINTRAC to make a disclosure. All such disclosures are approved by Mr. MacKillop or his Assistant Director.

Annette Ryan is Deputy Director of Partnership, Policy, and Analysis (“PPA”). Broadly speaking, the PPA Sector develops *strategic* intelligence, meaning intelligence that does not relate to particular individuals or entities. The PPA Sector identifies general trends, typologies, and emerging developments in money laundering and terrorist activity financing. Its role is essentially to integrate the work of three distinct units: strategic policy and reviews (“SPAR”); international relationships; and strategic intelligence, research, and analytics (“SIRA”). It also maintains a relationship with Finance in its role as the policy lead for the anti-money laundering and anti-terrorist activity financing regime.

Donna Achimov is Chief Compliance Officer and Deputy Director (Compliance). Ms. Achimov explained that the Compliance sector has a three-fold role. First, it engages in outreach and education with reporting entities, as well as industry and professional associations. The goal is to create a culture of compliance in which reporting entities understand their obligations and comply with them. Second, it examines reporting entities to assess their compliance. It uses a risk-based model to determine which entities should be examined in a given year. Third, it has enforcement capability. Depending on the level of non-compliance, it can take various actions, ranging from requiring reporting entities to develop an action plan to imposing administrative monetary penalties. Again, however, the emphasis is on fostering compliance, rather than punishment.

Limitations on panel members' evidence

The panel members noted that the *PCMLTFA* imposes statutory limitations on what they were able to discuss in the interview. Mr. MacKillop explained that the *PCMLTFA* imposes strict limits on the use that can be made of financial intelligence received by the Intelligence Sector. He stated that s. 55(1) of the *PCMLTFA* prohibits him from referring to any information that may directly or indirectly identify an individual who is the subject of a report or disclosure. As a result, he could not discuss any specific reports or disclosures made by FINTRAC. While he was able to provide some approximate numbers of disclosures or reports received, there too he had to be cautious.



FINTRAC's intelligence-gathering activities

The panel was asked to expand on how FINTRAC develops intelligence. Mr. MacKillop explained that the Intelligence Sector receives and assesses reports from reporting entities as well as VIRs. It cannot, however, proactively request information or conduct any investigations. It cannot ask reporting entities for a document or report relating to a particular individual or entity.

Mr. MacKillop noted that in preparing disclosures, the Intelligence Sector aims to provide as much information as it can to the recipient of the disclosure. It therefore consults other sources to corroborate the intelligence it receives from reports. These sources include some law enforcement databases, subscription services (such as ONCORP), and open source information. When asked when and how the Intelligence Sector chooses to consult open source information, Mr. MacKillop stated that it is disclosure driven. It may, for example, search the name of an individual to confirm that he or she is the director of a company.

Mr. MacKillop stated that the Intelligence Sector may also conduct its own research based on current events, which is part of situational awareness. For example, if an ideologically motivated attack occurred in another country, his team might search the names involved to see if there is a Canadian nexus. Mr. MacKillop noted that with the Convoy happening in Ottawa, it was incumbent on his unit to be aware of the names reported in the media to see if it had relevant information that would assist law enforcement or national security agencies and, if the threshold was met, make any relevant disclosures.

Mr. MacKillop noted that FINTRAC does *not* use any information that is illegally obtained. It did not, for example, make any use of the leaked GiveSendGo donor list. He added that FINTRAC did not receive the lists of individuals identified by law enforcement as being involved in protests and provided to financial institutions. [These lists were provided by the RCMP to a variety of financial institutions in order to assist the institutions in complying with their obligations under the *Emergency Economic Measures Order* (“EEMO”) to cease dealings with certain persons.]

Mr. MacKillop noted that the Intelligence Sector receives over 30 million transaction reports per year. This is in part due to a variety of “threshold” reports, in which reporting entities must report all transactions worth \$10,000 or more. FINTRAC maintains records of these reports for 10 years (or longer if there has been a disclosure). As a result, at any given time, FINTRAC's database has over 300 million transactions. Searching the database can therefore be challenging. Sometimes FINTRAC will ask reporting entities to flag suspicious transaction reports relating to a particular money laundering or terrorist financing concept, such that the report is flagged for early review by analysts. Ms. Ryan added that her team has an analytics lab populated by data scientists who can assist the Intelligence Sector with specific queries of the database; however, this is based on the “need to know” principle and is typically a “one-way street” in the sense



that her team does not hear from the Intelligence Sector about the specific nature of its analyses of suspicious transaction reports or the disclosures it is working on.

Mr. MacKillop noted that Intelligence Sector can also receive VIRs from law enforcement, national security agencies, and others. As the name suggests, such disclosures are made voluntarily, without a request from FINTRAC. He explained that FINTRAC is required to analyze every VIR it receives; however, FINTRAC does not acknowledge receipt of VIRs or follow-up with those who make VIRs about what it does with the intelligence. FINTRAC also has approximately 100 memoranda of understanding with financial intelligence units in other countries, which permit information sharing between the units where there is a nexus to a crime in another country.

Ms. Ryan explained that the PPA Sector's development of intelligence is complementary to, but distinct from, the work done by the Intelligence Sector. The PPA Sector's function is to maintain situational awareness: it determines whether new patterns are emerging, examines how the activity is happening, and shares that information with other sectors of FINTRAC. Her research teams follow developments in money laundering and terrorist financing activity and risks, including activity relating to "predicate offences" [which are offences that generate the funds that are then laundered]. To carry out this work, the PPA Sector looks at open source information including media sources, social media, some databases, specialist journals, and analytic sites and products. It also interacts with other domestic and international agencies about evolving trends, both in terms of activity being observed and approaches in the policy space.

Ms. Achimov noted that the Compliance team's education function also requires knowledge of trends and emerging patterns in order to educate reporting entities on indicators of suspicion. Educating reporting entities on such indicators leads to better quality reports. She noted that every sector has different risks; indicators of suspicion relating to casinos are different from those relating to financial institutions or accountants. The Compliance team interacts regularly with the PPA Sector, as well as with colleagues in the "Five Eyes" [an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States], provincial and federal regulators, and the Financial Action Task Force (FATF) [an international body that sets anti-money laundering and counter-terrorist financing standards] to exchange information about new and emerging risks.

[Part of FINTRAC's work involves maintaining a registry of money services businesses.]

Mr. MacKillop noted that the Compliance team can use law enforcement databases to verify whether applicants for registration as money services businesses have a criminal record, which would be grounds to deny or revoke a registration. It also assesses corporate organization structures to ensure there is some indication they are credible organizations operating legally.



Mr. MacKillop was asked how FINTRAC's work dovetails with the kind of analysis done by CSIS. He explained that FINTRAC is not responsible for identifying threats and individuals who are threats—that is done by CSIS and law enforcement. However, FINTRAC considers individuals identified by CSIS and law enforcement in VIRs, and, if the relevant threshold is met, makes disclosures based on that information. FINTRAC can also request permission to share information in a VIR with another law enforcement agency, in which case it would only share the information that FINTRAC itself has generated, not the original VIR.

Monitoring of the Convoy

[Documents produced by FINTRAC in January and February 2022 discuss the risks relating to crowdfunding services, payment service providers, cryptocurrency, and the financing of ideologically motivated violent extremism (IMVE).²] The panel was asked whether the Convoy was of interest to FINTRAC because of the potential that IMVE-related financing was occurring. Ms. Ryan stated that it was of potential interest for that reason, but that simply donating to a cause or organizing a protest does not amount to IMVE financing. When asked whether, in FINTRAC's view, IMVE-related financing always amounts to terrorist financing, Ms. Ryan responded that it does not. However, Mr. MacKillop indicated that FINTRAC is aware that extremist elements can use a non-violent group or activity for its own extremist agenda, and this potential is considered in the course of FINTRAC's work.

[A document dated January 26 produced by FINTRAC indicates that “[a]t this time, it is unclear whether the funds being raised through crowdfunding will be used specifically for violent extremist attacks, considering that all IMVE attacks in Canada have been low-cost and low in sophistication. The potential for the funds being used for violent activity seems unlikely at this time considering IMVE crowdfunding is usually not used towards conducting violent activity.”³] Ms. Ryan explained that this observation was based on general observations about crowdfunding and IMVE, rather than the Convoy specifically, noting that according to the literature, crowdfunding is not frequently used to fund IMVE.

[The document also indicates that SIRA was closely monitoring the events in partnership with the Intelligence Sector.⁴] Ms. Ryan explained that SIRA was doing

² See, for example, PB.CAN.00000017_REL.0001, SSM.NSC.CAN.00000081_REL.0001, SSM.NSC.CAN.00000111_REL.0001, SSM.NSC.CAN.00000119_REL.0001, SSM.NSC.CAN.00000120_REL.0001, PB.NSC.CAN.00000578_REL.0001.

³ PB.NSC.CAN.00000578_REL.0001, p 2.

⁴ PB.NSC.CAN.00000578_REL.0001, p 2.



some keyword searches of reports coming in and checking in with the Intelligence Sector to see what it would be helpful to monitor. Mr. MacKillop added that such monitoring and sharing of information is typical when events like these occur.

[An email from a FINTRAC analyst on January 27 compiled a list of individuals linked to the Convoy based on open source information.⁵] When asked why FINTRAC was tracking these individuals, Mr. MacKillop stated that this email was written by a member of the Intelligence Sector who was noting some people about whom there had been derogatory comments (with “derogatory” in this context meaning negative information about them, such as indications that they have incited violence, accepted money under false pretenses, etc.). He explained that FINTRAC would query its database in situations like this to see if it had any information about such individuals that could lead to a disclosure.

The panel was asked about a draft document from February 2 called “Terrorist Financing Risks of Freedom Convoy” whose stated purpose is to “provide background on the potential terrorist activity financing risks associated with the funding of the ‘Freedom Convoy.’”⁶ Ms. Ryan explained that this is an example of open source situational awareness: it was a draft prepared by a junior analyst at SIRA and sent to their team lead that attempts to summarize open source information to support further research and analysis. It was an assessment of the risk from a strategic view, that is, general patterns to be aware of as events continued. Mr. MacKillop added that this is the kind of analysis that FINTRAC does on a daily basis: it keeps track of events that have the potential to become violent in Canada and identifies people in its database who may be financing those activities. FINTRAC tries to act preventatively whenever possible: if it can help law enforcement *prevent* a violent event, that is FINTRAC’s goal.

When asked if FINTRAC had information suggesting that the border blockades (rather than the demonstrations in Ottawa) were being funded by crowdfunding campaigns, Mr. MacKillop stated that as crowdfunding services were not reporting entities prior to the *EEMO*, FINTRAC received no reports to this effect. To his recollection, media reporting was focusing on crowdfunding relating to the Ottawa demonstrations rather than the border blockades.

When asked about FINTRAC’s monitoring of the use of cryptocurrencies, Mr. MacKillop stated that cryptocurrencies are increasingly being used by criminals and criminal organizations to advance their activities. He noted that it was publicly known that there were cryptocurrency wallets [essentially virtual accounts that can receive and send cryptocurrency] to which the public could send virtual currency to support the Convoy.

⁵ PB.NSC.CAN.00000583_REL.0001, p 2.

⁶ SSM.NSC.CAN.0000078_REL.0001 is a covering email, and SSM.NSC.CAN.0000079_REL.0001 is the document.



As part of its triage, FINTRAC considered suspicious transaction reports from virtual currency dealers (which are reporting entities) that related to the Convoy demonstrations.

Ms. Ryan noted that cryptocurrencies have a considerable open source element in the sense that transactions on the blockchain [essentially a public ledger of cryptocurrency transactions] are publicly accessible.

Mr. MacKillop discussed the capabilities of FINTRAC in relation to monitoring cryptocurrency transactions.

Impact of the Emergency Economic Measures Order

Mr. MacKillop stated that there was no noticeable difference in the numbers of suspicious transaction reports that FINTRAC received between January 26 and February 23, 2022 relative to other periods. He noted that FINTRAC receives several thousand suspicious transaction reports per day. Between January 26 and February 23, it received fewer than 50 suspicious transaction reports relating to Convoy activity, and by the end of March, it had received fewer than 200 reports. (Ms. Paquet noted that the nature of FINTRAC's work is that it receives reports after the fact, so it received reports relating to that period after February 23.)

As for VIRs, Mr. MacKillop said that FINTRAC receives, on average, about 1700-1800 per year. Between January 26 and February 23, it received relatively few VIRs. Mr. MacKillop added that the low number of VIRs may be due in part to the fact that law enforcement was doing mostly frontline work rather than investigations.

Mr. MacKillop stated that FINTRAC similarly did not make more disclosures than usual during the January 26 to February 23 period.

Mr. MacKillop stated that when the *EEMO* came into effect and made crowdfunding and payment service providers reporting entities, this did not change the reporting patterns FINTRAC was seeing. Ms. Achimov explained that the period in which the *EEMO* was in force was too short for entities to complete the registration process; however, her sector "pre-registered" some entities, meaning they did enough to allow these entities to begin reporting without completing the whole registration process.

Ms. Paquet stated that FINTRAC was not involved in the drafting of the *EEMO*. FINTRAC was asked by the Department of Finance whether crowdfunding services were currently covered and, if not, what the best way to cover them would be; however, Finance remained the policy maker. She added that FINTRAC was involved in the



drafting of the regulations that later amended the *PCMLTFA* to make crowdfunding services and payment service providers reporting entities on a permanent basis.⁷

Ms. Paquet noted that there had been international reports since around 2017 suggesting that crowdfunding services be covered by anti-money laundering and counter-terrorist financing regimes. At one point, the FATF recommended it, and the director of the Financial Crimes Enforcement Network [FinCEN, the US equivalent of FINTRAC] was considering it. She explained that FINTRAC did not identify crowdfunding as a gap per se, but rather a potential vulnerability in the regime. She stated that Canada is now leading the way internationally by including these services in the *PCMLTFA*. Ms. Achimov added that it is common for Finance to add new reporting entities to the *PCMLTFA* regime, and that her team is accustomed to reaching out to new segments of the population that become subject to FINTRAC's oversight.

When asked whether the *EEMO* was useful for FINTRAC's ability to fulfil its mandate, Mr. MacKillop stated that from an intelligence perspective, it had no impact. The *EEMO* did not increase FINTRAC's authority or alter who could receive disclosures, and it was not in place long enough for FINTRAC to receive new reports from new reporting entities. He stated that it will become clear as FINTRAC receives more reports from crowdfunding entities and payment service providers how useful those reports are, including their quality and quantity. When asked whether, prior to the *EEMO*, Mr. MacKillop's team felt sufficiently equipped to fulfil its duties, he said that it did.

When asked what kind of feedback FINTRAC received from industry relating to the *EEMO*, Ms. Achimov stated that she did not hear concerns per se, but rather various questions about how it operated. For example, her sector received inquiries about whether the *EEMO* applied in a given situation, how to set up a reporting mechanism, and the like.

Ms. Paquet stated that FINTRAC did not provide input on when to revoke the *Emergencies Act*. She learned of the revocation from the media.

⁷ Canada Gazette, Part II, Vol 156, No 9, p 1166.